Michał MOSIĄDZ, Janusz SOBIECH, Jacek WÓJCIK
Główny Urząd Miar
Zakład Metrologii Interdyscyplinarnej

BEZPIECZEŃSTWO CYFROWE A RZETELNOŚĆ POMIARU

Zadaniem metrologii jest zapewnienie rzetelności i powtarzalności pomiarów. We współczesnych przyrządach pomiarowych za ten aspekt działania przyrządów pomiarowych odpowiedzialne jest oprogramowanie sterujące. Artykuł omawia regulacje bezpieczeństwa cyfrowego przyrządów pomiarowych i inne zagadnienia związane z ryzykiem obniżenia wiarygodności pomiarów i wystąpienia incydentów bezpieczeństwa informatycznego.

Słowa kluczowe: rzetelność pomiaru, bezpieczeństwo cyfrowe, software

Cyfryzacja życia społecznego i gospodarczego wiąże się z rozwojem urządzeń cyfrowych upraszczających codzienne czynności i wspomagających procesy przemysłowe. Postęp techniczny wymusza rozwój i standaryzację komunikacji cyfrowej człowieka z maszyną oraz pomiędzy urządzeniami. Kolejne etapy rozwoju techniki przekształciły niezależne, proste urządzenia analogowe w złożone środowiska urządzeń elektronicznych, które bez udziału człowieka współpracują ze sobą (np. *Internet of Things* (IoT)). Proces budowy rozproszonych systemów informatycznych objął również przyrządy pomiarowe. Coraz częściej – zarówno w codziennym życiu, jak i w nowoczesnych laboratoriach metrologicznych – spotykamy złożone sieci współpracujących ze sobą przyrządów pomiarowych. Jako przykłady mogą tu służyć inteligentne sieci mierników mediów komunalnych (*smart-grids* i *smart-meters*), rozproszone systemy teleinformatyczne przeznaczone do wyznaczania skali czasu UTC, nawigacji satelitarnej oraz inne zaawansowane układy pomiarowe.

Pozornie odległe obszary metrologii łączy dążenie do uzyskania najlepszej możliwej rzetelności i wiarygodności pomiarów. Wskutek rozwoju technologii nie wystarczają dotychczasowe procedury oparte na okresowej konserwacji wzorców i przyrządów pomiarowych, oraz wiedzy i doświadczeniu osoby dokonującej pomiaru i przetwarzającej jego wyniki. Wobec cyfryzacji procesów metrologicznych niezbędne stało się stworzenie zbioru standardów technologicznych zapewniających wiarygodność i bezpieczeństwo pomiarów. Są one fundamentem zaufania do wyników pomiarowych i zapewniają ich wiarygodność w obliczu możliwości przekłamania danych cyfrowych będących skutkiem niedoskonałości techniki, ludzkiej nieuwagi bądź celowej manipulacji.

1. RZETELNOŚĆ NOWOCZESNYCH UKŁADÓW POMIAROWYCH

Przyrządy pomiarowe można grupować m.in. ze względu na obszar ich zastosowania albo stopień ich złożoności – od prostych, niezależnych przyrządów pomiarowych (analogowych i cyfrowych), poprzez sieci współpracujących ze sobą przyrządów o architekturze zamkniętej, po przyrządy rozproszone i wirtualne. Każde urządzenie pomiarowe można przedstawić jako układ współpracujących elementów obejmujących czujnik pomiarowy, układ przetwarzania danych i element wskazujący wynik. Określenie to długo wystarczało nawet dla rozbudowanych układów pomiarowych składających się ze skomplikowanych podzespołów sterowania, pomiaru i regulacji. Mimo zaawansowania technologicznego jak np. w układach odtwarzania jednostek miar wykorzystujących zjawiska kwantowe – wiarygodność pomiaru oparta jest zwykle na doświadczeniu i wiedzy operatora układu pomiarowego.

Zmiany technologiczne, w tym technologie telekomunikacyjne umożliwiły wymianę i przetwarzanie ogromnych ilości danych (tzw. *Big Data*) powodując zmiany konstrukcji przyrządów. Obserwujemy odejście od konstrukcji przyrządu pomiarowego, w którego obudowie zamknięte są podzespoły umożliwiające pomiar i prezentację wyniku. Pojawiają się przyrządy wirtualne i rozproszone oraz możliwości sterowania elementami układów pomiarowych w oddalonych lokalizacjach (np. kosmicznych stacjach badawczych), układy rozproszonego przetwarzania danych (tzw. chmura obliczeniowa, współdzielenie zasobów). Użycie Internetu pozwala przesłać wyniki pomiaru na urządzenie mobilne, które nie jest bezpośrednio związane z urządzeniem pomiarowym. W ten sposób granica między przyrządem i układem pomiarowym ulega zatarciu, co uzasadnia konieczność redefinicji pojęcia przyrządu pomiarowego i uwzględnienia specyfiki przyrządów wirtualnych i rozproszonych.

Nowego podejścia wymagają zagadnienia związane z zapewnieniem wiarygodności i bezpieczeństwa pomiaru. Zbiór zasad zapewniających rzetelność w metrologii musi obejmować: powtarzalność procedury i warunków pomiaru, poprawność odczytu wskazań, prawidłowy dobór metodyki analizy wskazań, poprawną metodykę dalszego przetwarzania danych.

W ujęciu metrologii analogowej wystarczająca była kontrola warunków środowiskowych. Patrząc szerzej na proces pomiarowy, należy pod pojęciem środowiska pomiaru rozumieć również powtarzalność wyposażenia pomiarowego, obejmującą niezmienność konfiguracji przyrządów pomiarowych. Środowisko pomiarowe można zdefiniować jako zbiór warunków środowiskowych i sprzętowych zapewniających powtarzalność przebiegu pomiaru. We współczesnych układach tradycyjnie rozumiany przyrząd pomiarowy można ograniczyć do układu czujnika wraz z układem formującym sygnał wyjściowy. Nie można jednak pominąć roli oprogramowania, którego jakością i stabilnością działania jest zdeterminowany przebieg procesu pomiarowego. Proces pomiarowy zależy od głównego programu sterującego i środowiska jego pracy (w tym: systemu operacyjnego, BIOS-u, sterowników, podzespołów, interfejsów komunikacyjnych). Brak nadzoru nad wszystkimi elementami i poprawnością ich funkcjonowania może prowadzić do zaburzenia pomiaru i utraty wiarygodności wyników. W procesach pomiarowych wymagających szczególnych warunków technologicznych (np. warunki próżniowe, kriogeniczne) przy sytuacjach nietypowych brak właściwej kontroli może doprowadzić do zagrożeń dla unikatowego wyposażenia pomiarowego i personelu. Konieczne jest uwzględnianie stabilności całego środowiska sprzętowego pomiaru i wprowadzenie rozwiązań wspomagających zarządzanie wersjami oprogramowania metrologicznego. Postęp techniki komputerowej sprawił, że w epoce pracy sieciowej niemożliwe jest zapewnienie niezmienności oprogramowania poprzez odpięcie sieci komputerowych.

Kolejnym zagadnieniem mającym wpływ na rzetelność wyników pomiaru są zasady postępowania z danymi pomiarowymi w zakresie ich przetwarzania i ochrony. Przetwarzanie danych obejmuje cały proces, począwszy od rejestracji wyników poprzez wykonanie niezbędnych obliczeń, po analizę uzyskanych wartości i wyznaczenie niepewności pomiaru. Ochrona danych musi obejmować całą ścieżkę ich przetwarzania. Konieczne jest określenie wyraźnej granicy – gdzie kończy się rola regulacji metrologicznych w zakresie ochrony danych, a także – redefinicja przyrządu pomiarowego.

Niektórzy zainteresowani chcieliby ograniczyć regulacje do części stricte metrologicznej przyrządu, związanej bezpośrednio z pomiarem wielkości fizycznej. Inni mając podejście bardziej holistyczne definiują granice regulacji metrologicznych w odniesieniu do chwili wygenerowania wyjściowego wyniku jako ostatecznego celu pomiaru. Przykładowo: całkowite zużycie energii dla liczników energii elektrycznej albo wygenerowanie danych (zdjęć) stanowiących dowód wykroczenia w ruchu drogowym, a nie tylko wartość zmierzonej przed czujnik prędkości.

Podobnie rzecz ma się z definicją prezentacji danych. W epoce powszechnego przesyłu danych i ich przetwarzania w chmurze należy określić czy i kiedy wskazanie przyrządu jest wiarygodne: czy tylko na wyświetlaczu urządzenia pomiarowego? poprzez odtworzenie z chronionego pliku za pomocą dedykowanego oprogramowania w urządzeniu mobilnym? w momencie transmisji

z urządzenia w postaci cyfrowej? Są to podstawowe pytania, na które dzisiaj metrologia musi znajdować odpowiedzi. W tym zadaniu wsparciem dla metrologii są ogólne zasady bezpieczeństwa danych cyfrowych, które obejmują: analizę ryzyka informatycznego, metody uwierzytelniania danych oraz procedury postępowania, monitorowania i dostępu do systemów. Zabezpieczenia i procedury są niezbędne, gdyż bezpieczne dane to wiarygodne dane.

2. BEZPIECZEŃSTWO CYFROWE W WYMAGANIACH METROLOGICZNYCH

Obszary ryzyk bezpieczeństwa informatycznego, istotne dla zapewnienia dużej jakości pomiarów, zostały dostrzeżone przez środowisko metrologiczne i obejmują niezmienność środowiska programowego pomiaru, wiarygodność wyników i odtwarzalność ścieżki ich przetwarzania i transmisji, zarządzalność zmianami oprogramowania, kontrolę wpływu innego oprogramowania pracującego w układzie pomiarowym oraz obsługę sytuacji awaryjnych i wyjątków.

Tabela 1

Obszary regulacji i wpływ na wiarygodność

WYMAGANIA SZCZEGÓŁOWE W OBSZARACH REGULACJI	WPŁYW NA WIARYGODNOŚĆ Cel regulacji
BEZPIECZEŃSTWO OPROGRAMOWANIA – Jednoznacznie identyfikowalne oprogramowanie – Niezależność programu sterującego od innego oprogramowania	OPROGRAMOWANIE Niezmienność programu
– Automatyczna aktualizacja oprogramowania z zachowaniem zabezpieczeń – Autoryzacja autentyczności i sprawdzenie integralności aktualizacji – Nieusuwalny rejestr zmian oprogramowania	Zarządzanie aktualizacjami
– Zabezpieczenie przed przypadkowymi zmianami i celową modyfikacją	DANE – Niezmienność
– Brak możliwości zmiany i wiarygodna prezentacja wyników – Rozróżnienie wyników pomiaru od informacji dodatkowych	INTERFEJSY Interfejs użytkownika (GUI)
– Brak wpływu na zawartość i działanie programu, konfigurację i dane – Bezpieczna wymiana danych metrologicznych	Zabezpieczenie interfejsów i komunikacji
– Inne oprogramowanie nie może zaburzać pomiaru – Ciągłość pracy programu w sytuacjach awaryjnych i zaburzeń działania – Wewnętrze zasilanie zapewniające odpowiednio długą ciągłą pracę	POMIAR Odporność na awarie
– Zabezpieczenie przed nieautoryzowaną zmianą	Parametry konfiguracyjne
BEZPIECZEŃSTWO PRZECHOWYWANIA DANYCH – Przechowywanie wszystkich wymaganych danych Zabezpieczenie przed przypadkowymi zmianami i celową modyfikacją	DANE Zapewnienie niezmienności danych
– Zachowane dane zapewniają identyfikowalność pomiaru – Poufność kluczy kryptograficznych i zabezpieczonych danych	Poufność i uwierzytelnienie danych
– Prezentacja i weryfikacja niezmienności zapisanych danych – Automatyczny zapis i odpowiednia pojemność nośnika danych – Okresowa kopia zapasowa danych pomiarowych w pamięci nieulotnej – Brak możliwości skasowania liczników kumulacyjnych	Odtwarzalność danych
– Zapewnienie ciągłego i poprawnego wskazywania wyniku pomiaru	INTERFEJS (GUI)
– Wykrywanie i raportowanie przekroczenia parametrów pracy	POMIAR – Niezawodność
BEZPIECZEŃSTWO TRANSMISJI DANYCH – Przesyłanie wszystkich niezbędnych danych do dalszego przetwarzania – Zabezpieczenie transmitowanych danych przed przypadkowymi zmianami – Zabezpieczenie przed celową modyfikacją przesyłanych danych	DANE Zapewnienie niezmienności danych
– Weryfikacja autentyczności przesyłanych danych Poufność kluczy kryptograficznych i zabezpieczonych danych	Poufność i uwierzytelnienie danych
– Obsługa i uniemożliwienie przetwarzania uszkodzonych danych – Opóźnienie transmisji nie może wpływać na przebieg pomiaru – Zachowanie danych w przypadku niedostępności sieci komunikacyjnej	POMIAR Niezawodność i odporność na awarie

Dla podniesienia poziomu bezpieczeństwa metrologicznego, zarówno w obszarze handlu, technologii i badań naukowych opracowano szereg zbiorów wymagań, wytycznych i norm bezpieczeństwa ICT w zastosowaniach metrologicznych. Wśród nich należy wyszczególnić zasady zawarte w regulacjach prawnych oraz opracowaniach organizacji metrologicznych (OIML, WELMEC) i jednostek normalizacyjnych (PKN), takich jak: Dyrektywa MID [2], Dyrektywa NAWI [1], OIML D31 [3]; przewodnik WELMEC 7.2 [4], normy branżowe dotyczące urządzeń pomiarowych (np. dla wag nieautomatycznych PN-EN 45501), przepisy dotyczące wymagań technicznych dla poszczególnych rodzajów przyrządów pomiarowych (np. Rozporządzenie Ministra Gospodarki z dnia 17 lutego 2014 r. w sprawie wymagań, którym powinny odpowiadać przyrządy do pomiaru prędkości pojazdów w ruchu drogowym, oraz szczegółowego zakresu badań i sprawdzeń wykonywanych podczas prawnej kontroli metrologicznej tych przyrządów pomiarowych). Zarys wymagań w poszczególnych obszarach regulacji i ich znaczenie dla wiarygodności pomiaru prezentuje tabela 1. Kolejne aktualizacje omawianych wytycznych zawierają coraz bardziej szczegółowe wymagania w zakresie bezpieczeństwa ICT wynikające z postępu techniki. Wśród producentów przyrządów pomiarowych i w środowiskach naukowych obecna jest tendencja do szybkiego wdrażania nowoczesnych rozwiązań technicznych. Jako przykłady można wymienić technologie mobilne i przetwarzanie danych oparte o zbiory typu *BigData*.

PODSUMOWANIE

Coraz częściej w przyrządach pomiarowych stosuje się oprogramowanie metrologiczne. Rozwój technologii sprawił, że dawne metody zapewnienia rzetelności pomiaru są niewystarczające. Metrologia w urządzeniach informatycznych używa metod i zabezpieczeń przetwarzania i ochrony danych stosowanych w innych dziedzinach teleinformatyki. Specyfika zagadnień metrologicznych wymusza definiowanie szczegółowych wymogów dla rozwiązań informatycznych w urządzeniach pomiarowych. Poza regulacjami prawnymi wymagania dla przyrządów zawierających oprogramowanie są uściślane poprzez działalność międzynarodowych organizacji metrologicznych, które wypracowują uznane i stosowane wytyczne w celu zwiększenia poziomu bezpieczeństwa informatycznego i zapewnienia najwyższej wymaganej jakości pomiarów w nowoczesnych laboratoriach pomiarowych.

LITERATURA

[1] *Dyrektywa Parlamentu Europejskiego i Rady 2014/31/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku wag nieautomatycznych*.
[2] *Dyrektywa Parlamentu Europejskiego i Rady 2014/32/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych*.
[3] *General requirements for software controlled measuring instruments*, OIML D 31, 2008 (E).
[4] *WELMEC 7.2, 2015: Software Guide* (Measuring Instruments Directive 2014/32/EU), European Cooperation in Legal Metrology.